IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: David E. MCDYSAN	
Application No.: 10/023,043	Group Art Unit: 2135
Filed: December 17, 2001	Examiner: Gyorfi, T.
Customer No.: 25537 Attorney Docket: RIC01059 Client Docket: 09710_1203	

For: SYSTEM, METHOD AND APPARATUS THAT EMPLOY VIRTUAL PRIVATE NETWORKS TO RESIST IP QoS DENIAL OF SERVICE ATTACKS

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated December 26, 2006.

I. REAL PARTY IN INTEREST

The real party in interest is WORLDCOM, Inc.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related Appeal or Interference.

III. STATUS OF THE CLAIMS

Claims 1 through 24 are pending in this Application and have been finally rejected.[12] It is from the Final Office Action dated July 24, 2006 that this Appeal is taken.

Claims 1 through 3, 7 through 11, 14 through 17, and 19 through 24 were previously presented; claims 4 through 6, 12, 13, and 18 are original claims.

IV. STATUS OF AMENDMENTS

No Amendment has been submitted subsequent to the issuance of the Final Office Action dated July 24, 2006. A response pursuant to 37 C.F.R. § 1.116 (Request for Reconsideration) was submitted on September 25, 2006, in which none of the claims were amended. According to the Advisory Action dated October 12, 2006, the September 25, 2006 response would be entered for purposes of appeal.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Independent Claim 1.

Independent claim 1 is directed to a network system providing a virtual private network (VPN) (see, e.g., paragraph [25], lines 3-5; FIG.3, element 20). The claimed network system comprises one or more egress routers (see, e.g., paragraph [26], lines 3-5; FIG.3, elements 24a and 25a) having connections to an access network including an access link (see, e.g., paragraph [26], line 7 and paragraph [27], lines 5-7) wherein one or more egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first access network logical connection for intra-VPN traffic (see, e.g., paragraph [26], lines 10-12)

[1] The claims in this case have been rejected no less than seven times, including three final rejections.

and all extra-VPN traffic to the destination host from sources outside the VPN within a second access network logical connection for extra-VPN traffic (see, e.g., paragraph [26], lines 11-12), the second access network logical connection being separate and apart from the first access network logical connection (see, e.g., paragraph [27], lines 4-5). The claimed network system also comprises a plurality of ingress routers (see, e.g., paragraph [26], lines 3-5 and paragraph [25], lines 8-9; FIG. 3, elements 24b, 24c and 24d) coupled to one or more egress routers (see, e.g., paragraph [26], lines 2-4 and paragraph [25], lines 8-9; FIG.3, elements 24a and 25a) for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN, such that denial of service attacks on the access link originating from sources outside the VPN are prevented (see, e.g., paragraph [26], lines 10-12).

Independent Claim 9.

Independent claim 9 is directed to a network system, comprising an access network having an access link to a destination host belonging to a VPN (see, e.g., paragraph [27], lines 4-5), wherein the access network supports a first logical connection for intra-VPN traffic from sources within the VPN (see, e.g., paragraph [26], lines 9-10) and a second logical connection for extra-VPN traffic from sources outside the VPN (see, e.g., paragraph [26], lines 11-12), one or more egress routers having connections to the access network, wherein said one or more egress routers transmit intra-VPN traffic to the destination host via the first logical connection and all extra-VPN traffic to the destination host via the second logical connection (see, e.g., paragraph [27], lines 10-13), and a plurality of ingress routers (see, e.g., paragraph [26], lines 3-5 and paragraph [25], lines 8-9; FIG.3, elements 24b, 24c and 24d) coupled to one or more egress

routers (see, e.g., paragraph [26], lines 2-4 and paragraph [25], lines 8-9; FIG.3, elements 24a and 25a) for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented (see, e.g., paragraph [27], lines 11-16).

Independent Claim 16.

Independent claim 16 is directed to a method of providing a VPN, which method comprises providing a first logical connection for intra-VPN traffic from sources within the VPN in an access network (see, e.g., paragraph [26], lines 10-12) and a second logical connection for extra-VPN traffic from sources outside the VPN (see, e.g., paragraph [26], lines 11-12), communicating, from a plurality of ingress routers to one or more egress routers, intra-VPN and extra-VPN traffic destined for a destination host belonging to the VPN (see, e.g., paragraph [26], lines 1-5), wherein the intra-VPN traffic and extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (see, e.g., paragraph [26], lines 10-12 and [27], lines 4-5), and transmitting intra-VPN traffic from said one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers to the destination host via the second logical connection, such that denial of service attacks on the access link originating from sources outside the VPN are prevented (see, e.g., paragraph [27], lines 10-19).

Independent Claim 21.

Independent claim 21 is directed to a method of providing a VPN, the method comprising assigning a first priority level to intra-VPN traffic flowing from sources within the VPN and

assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN (see, e.g., paragraph [27], lines 4-5), granting precedence to traffic having the first priority level at the access link to a destination host belonging to the VPN over traffic having the second priority level (see, e.g., paragraph [27], lines 6-10), and transmitting the intra-VPN traffic from one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers to the destination host via a second logical connection (see, e.g., paragraph [27], lines 10-19).

Independent Claim 22.

Independent claim 22 is directed to a communication method, the method comprising receiving a packet that is destined to a host within a virtual private network (see, e.g., paragraph [25], lines 3-5), determining whether the packet originated within the VPN or external to the VPN (see, e.g., paragraph [27], lines 1-5) and forwarding the packet to the host over a first logical path or a second logical path based upon the determination, wherein the first logical path is designated for traffic originating within the VPN and the second logical path is designated for traffic originating external to the VPN (see, e.g., paragraph [26], lines 10-13 and [27], lines 11-13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 3 through 9, 11 through 16, and 18 through 22 stand finally rejected under 35 U.S.C. § 102 for lack of novelty as evidenced by Seid et al.;

2. Claim 23 stands finally rejected under 35 U.S.C. § 103 for obviousness predicated upon Seid et al.; and

3. Claims 1 through 24 stand finally rejected under 35 U.S.C. § 103 over acknowledged prior art in view of Seid et al.

VII. ARGUMENT

Grouping of Claims.

For the convenience of the Honorable Board of Patent Appeals and Interferences (the "Board"), Appellant does not separately argue the patentability of any dependent claim. Appellant notes the pivotal issue involved in this appeal is common to all independent claims and, therefore, Appellant will not argue any independent claim separately. Accordingly, all of the appealed claims stand or fall together as a group with exemplary independent claim 1. Appellant will only separately argue the patentability of claim 1.

1. The rejection of claims 1, 3 through 9, 11 through 16, and 18 through 22 under 35 U.S.C. § 102 for lack of novelty as evidenced by Seid et al.

The factual determination of lack of novelty under 35 U.S.C. § 102 requires the identical disclosure in a single reference of each element of a claimed invention, such that the identically claimed invention is placed into the recognized possession of one having ordinary skill in the art. *Dayco Prods., Inc. v. Total Containment, Inc., 329 F.3d 1358, 66 USPQ2d 1801 (Fed. Cir. 2003); Crown Operations International Ltd. v. Solutia Inc., 289 F.3d 1367, 62 USPQ2d 1917 (Fed. Cir. 2002).* When imposing a rejection under 35 U.S.C. § 102 for lack of novelty, the Examiner is required to specifically identify wherein an applied reference is asserted to identically disclose each and every feature of a claimed invention, particularly when such is not apparent as in the present case. *In re Rijckaert, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993);*

Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co., 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984). That burden has not been discharged. Indeed, there is a fundamental difference between the claimed inventions and the apparatus and method disclosed by Seid et al. that scotches the factual determination that Seid et al. disclose an apparatus and method identically corresponding to those claimed.

Specifically, the network system defined in independent claim 1 comprises, *inter alia*, first and second access network logical connections. The first access network logical connection is for intra-VPN traffic. The second access network logical connection is for extra-VPN traffic. The second access network logical connection is separate and apart from the first access network logical connection. Both are within the VPN.

The claimed invention further comprises a plurality of ingress routers coupled to egress routers for communication utilizing the network-based VPN protocol that logically **partitions** intra-VPN and extra-VPN traffic, such that denial of service attacks on the access link originating from sources outside the VPN are prevented. **In other words, traffic in a particular VPN is separated or partitioned based on the source of the traffic, i.e., whether the traffic originated within the VPN (intra-VPN) or outside of the VPN (extra-VPN).**

Appellant emphasizes that the claimed systems and methods require the **strategic partitioning** of traffic originating within the VPN (intra-VPN traffic) from traffic originating without the VPN (extra-VPN traffic), and transmitting the intra-VPN and extra-VPN to **different** access network logical connections within the VPN to prevent denial of service attacks on the access link originating from sources outside the VPN. This concept is neither disclosed nor suggested by Seid et al.

The Examiner's Position.

In the exposition of the rejection appearing under the fifth enumerated section on page 4 of the July 24, 2006 Final Office Action, the Examiner asserted that Seid et al. disclose a network system corresponding to that claimed wherein intra-VPN traffic and extra-VPN traffic are routed to different access network logical connections, and a plurality of ingress routers coupled to egress routers utilizing a protocol that logically partitions intra-VPN and extra-VPN traffic to prevent denial of service attacks on the access link originating from sources outside the VPN. **Where? If only saying so could make it so.**

Appellant submits that the Examiner's analysis of Seid et al. does not even come within shouting distance of what Seid et al. actually disclose. There is a great disparity between what the Examiner says Seid et al. teach and what Seid et al. actually teach.

Specifically, the Examiner referred to column 4, lines 1 through 10, asserting the disclosure of separating intra-VPN from extra-VPN traffic. In column 4, lines 1 through 10, Seid et al. disclose that their improvement over the prior art provides for identification of packets on the network to specific VPNs, so that the level of service within a particular VPN is generally unperturbed by traffic generated by users outside the VPN's logical domain. In other words, packets to different VPNs are specifically identified, but **not** on the basis of whether they originated within a particular VPN or without a particular VPN, as in the claimed invention.

The Examiner also referred to column 2, line 56 through column 3, line 15. In the paragraph bridging columns 2 and 3 of Seid et al., it is disclosed that a VPN is a collection of logical nodes and virtual paths (VPs) and one or more virtual circuits (VCs), each VC being a logical connection between VC terminators and customer premises equipment. It is also disclosed that each VP is allocated at positive guaranteed bandwidth and each VC on a VP is also

allocated a bandwidth greater than or equal to zero. In this manner packets of information to be transmitted over a VC are provided with an address field having local significance for identifying the respective VCs and VPs used by **the** VPN to which the packets of information are associated. This is how congestion control of the network is provided on a per VPN basis, such that congestion outside of a particular VPN's logical domain does not affect the performance of the particular VPN.

Nowhere, repeat **nowhere**, do Seid et al. disclose or suggest the notion of partitioning or segregating traffic from sites within the same VPN (intra-VPN traffic) from traffic without that VPN (extra-VPN traffic), and applying a protocol that prioritizes intra-VPN traffic over extra-VPN traffic, or allocates access link capacity such that extra-VPN traffic cannot interfere with intra-VPN traffic. Indeed, in the ultimate sentence of paragraph 27 [paragraph 27] of the written description of the specification, Appellant disclosed that the conventional Diffserv and CPE edge router IP sec-based IP VPN implementations **do not segregate traffic destined for sites within the same VPN (i.e., intra-VPN traffic) and traffic sent from other regions of the Internet (i.e., extra-VPN traffic). This same originally disclosed distinction over the prior art applies to Seid et al.**

In the Advisory Action dated October 12, 2006, in the second paragraph of the continuation sheet, the Examiner responded to Appellant's arguments by asserting:

> Examiner notes that Seid teaches that each and very VPN managed by Seid is protected on a per-VPN basis against being impacted by traffic from outside its logical domain (Seid col. 3, lines 10 through 15).

But the Examiner does not go on to mention **how** this congestion control is implemented. Upon reading that entire paragraph, from which the Examiner surgically extracted lines 10 through 15 of column 3, one having ordinary skill in the art is informed that control is achieved

by allocating certain bandwidths among each VP and VC, and identifying packets of information over a VC with an address field having local significance for identifying the respective VCs and VPs used by the VPN to which the packets of information are associated. **Nothing, repeat nothing, is said about segregating, within the same VPN, intra-VPN traffic from extra-VPN traffic.**

The Examiner's rush to judgment based upon the disclosed congestion control within a particular VPN of Seid et al. ignores the fact that Seid et al. neither disclose nor suggest the concept of segregating intra-VPN traffic from extra-VPN traffic destined for sites within the same VPN. Instead of facing up to that fact, the Examiner attempts to misdirect attention to the overall objective of Seid et al. which is to control congestion within each VPN. Neither this misdirection nor any amount of airbrushing can bring about the requisite prior art revisionism to support the factual determination of lack of novelty under 35 U.S.C. §102.

The above argued disparity between what the Examiner says Seid et al. disclose and what Seid et al. actually disclose, which is a fundamental difference between the claimed invention and Seid et al., undermines the factual determination that Seid et al. disclose a system or method identically corresponding to those claimed. *Minnesota Mining & Manufacturing Co. v. Johnson & Johnson Orthopaedics Inc., 976 F.2d 1559, 24 USPQ2d 1321 (Fed. Cir. 1992); Kloster Speedsteel AB v. Crucible Inc., 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986).* In short, Seid et al. merely distinguish VPNs to isolate traffic from one VPN to another VPN to control congestion. Seid et al. neither disclose nor suggest the use of one or more egress routers that transmit intra-VPN traffic to a destination host belonging to a particular VPN from sources within the VPN within a first access network logical connection for intra-VPN traffic, and all extra-VPN traffic to the destination host from sources outside the VPN within a second access

network logical connection for extra-VPN traffic, to prioritize intra-VPN traffic over extra-VPN traffic, thereby preventing denial of service attacks on the access link originating from sources outside the VPN.

The above argued fundamental difference between the claimed inventions and Seid et al. undermine the factual determination that Seid et al. disclose a system or apparatus identically corresponding to those claimed. *Minnesota Mining & Manufacturing Co. v. Johnson & Johnson Orthopaedics Inc., supra; Kloster Speedsteel AB v. Crucible Inc., supra.* Appellant, therefore, submits that the imposed rejection of claims 1, 3 through 9, 11 through 16, and 18 through 22 under 35 U.S.C. § 102 for lack of novelty as evidenced by Seid et al. is not factually viable.

2. The rejection of claim 23 under 35 U.S.C. § 103 for obviousness predicated upon Seid et al.

As previously noted, Appellant does not separately argue the patentability of claim 23. Claims 1 through 24 stand or fall together as a group with exemplary claim 1.

3. The rejection of claims 1 through 24 under 35 U.S.C. § 103 for obviousness predicated upon the acknowledged prior art in view of Seid et al.

Appellant again notes that claims 1 through 24 stand or fall together as a group with exemplary independent claim 1. The Examiner admits that the acknowledged prior art does not disclose the concept of separating intra-VPN and extra-VPN traffic into first and second logical connections, and partitioning these logical connections such that denial of service attacks on the access link originating from sources outside the VPN are prevented. However, the Examiner

asserted that such a concept is disclosed by Seid et al. and then announced the obviousness conclusion.

Appellant incorporates herein the arguments previously advanced in traversing the imposed rejection of claim 1 under 35 U.S.C. § 102 for lack of novelty as evidenced by Seid et al. Suffice it to say, the acknowledged prior art does not cure the previously argued deficiencies of Seid et al. Accordingly, even if the acknowledged prior art is somehow combined with Seid et al., and Appellant does not agree that the requisite fact-based motivation has been established, the claimed invention would not result. *Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988)*. This is because Seid et al. neither disclose nor suggest the concept of partitioning intra-VPN traffic from extra-VPN traffic into first and second separate logical connections to prevent denial of service attacks on the access link originating from sources outside the VPN.

Appellant, therefore, submits that the imposed rejection of claims 1 through 24 under 35 U.S.C. § 103 for obviousness predicated upon the acknowledged prior art in view of Seid et al. is not factually or legally viable and, hence, solicit withdrawal thereof.

VIII. PRAYER FOR RELIEF

Based upon the arguments submitted *supra*, Appellant submits that the Examiner's rejections under 35 U.S.C. § 102 and 35 U.S.C. § 103 are not factually or legally viable. Appellant, therefore, solicits the Honorable Board to reverse each of the Examiner's rejections.

Respectfully submitted,

DITTHAVONG MORI & STEINER, P.C.

2/16/2007
Date

Sangwon S. Kim
Registration No. 54,221

for

Arthur S. Steiner
Attorney for Applicant
Registration No. 26,106

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9954
Fax. 703-519-9958

IX. CLAIMS APPENDIX

1. A network system providing a virtual private network (VPN), said network system comprising:

one or more egress routers having connections to an access network including an access link, wherein said one or more egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first access network logical connection for intra-VPN traffic and all extra-VPN traffic to the destination host from sources outside the VPN within a second access network logical connection for extra-VPN traffic, separate from the first access network logical connection; and

a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented.

2. The network system of Claim 1, wherein the at least one of the plurality of ingress routers or the at least one of the one or more egress routers logically partitions intra-VPN traffic and extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

3. The network system of Claim 1, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers.

4. The network system of Claim 1, and further comprising the access network.

5. The network system of Claim 4, and further comprising a customer premises equipment (CPE) edge router to the access link.

6. The network system of Claim 5, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

7. The network system of Claim 1, wherein at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic.

8. The network system of Claim 1, wherein said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic.

9. A network system, comprising:

an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

one or more egress routers having connections to the access network, wherein said one or more egress routers transmit intra-VPN traffic to the destination host via the first logical connection and all extra-VPN traffic to the destination host via the second logical connection; and

a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic,

such that denial of service attacks on said access link originating from sources outside the VPN are prevented.

10. The network system of Claim 9, wherein the at least one of the plurality of ingress routers or the at least one of the one or more egress routers logically partitions the intra-VPN traffic and the extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

11. The network system of Claim 9, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers.

12. The network system of Claim 9, and further comprising a customer premises equipment (CPE) edge router to the access link.

13. The network system of Claim 12, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

14. The network system of Claim 9, wherein at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic.

15. The network system of Claim 9, wherein said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic.

16. A method providing a virtual private network (VPN), said method comprising:

in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

communicating, from a plurality of ingress routers to one or more egress routers, intra-VPN and extra-VPN traffic destined for a destination host belonging to the VPN, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic;

transmitting intra-VPN traffic from said one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers to the destination host via the second logical connection, such that denial of service attacks on said access link originating from sources outside the VPN are prevented.

17. The method of Claim 16, wherein a Differentiated Services protocol is used to logically partition the intra-VPN traffic and the extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

18. The method of Claim 16, wherein a customer premises equipment (CPE) edge router is coupled between said access network and said destination host, said method further comprising:

at a physical port of the CPE edge router coupled to the access link, providing first and second logical ports; and

receiving intra-VPN traffic at the first logical port, and receiving extra-VPN traffic at the second logical port.

19. The method of Claim 16, and further comprising logically partitioning intra-VPN and extra-VPN traffic by at least one of said plurality of ingress routers utilizing a plurality of tunnels.

20. The method of Claim 16, and further comprising said one or more egress routers providing a plurality of different qualities of services to said intra-VPN traffic.

21. A method for providing a virtual private network (VPN), the method comprising:

assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN;

assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN;

granting, to traffic having the first priority level at the access link, precedence of access to a destination host belonging to the VPN over traffic having the second priority level; and

transmitting the intra-VPN traffic from one or more egress routers to the destination host via a first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers to the destination host via a second logical connection.

22. A method of communicating, comprising:

receiving a packet that is destined to a host within a virtual private network;

determining whether the packet is originated within the virtual private network or external to the virtual private network; and

forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the

virtual private network and the second logical path is designated for traffic originating externally to the virtual private network.

23. The method of Claim 22, wherein the packet is an Internet Protocol (IP) packet, and the steps of receiving, determining and forwarding are performed at a customer premises router configured to process the IP packet.

24. The method of Claim 22, wherein the packet over the first logical path is marked as a higher priority than the second logical path using a differentiated services protocol.

X. EVIDENCE APPENDIX

Not Applicable.

XI. RELATED PROCEEDINGS APPENDIX

Not Applicable.